IN THE CLAIMS

Please amend the claims as follows:

1. (Previously Presented) A device for managing network traffic flow, the device comprising:

a first processor, the first processor configured to

receive network traffic content,

determine whether a protocol of the network traffic content matches a prescribed protocol of network traffic content that could contain content desired to be detected by comparing a type of the network traffic content with a prescribed type,

store the network traffic content in a stack when the protocol of the network traffic content matches the prescribed protocol, and

perform filtering of the network traffic if the type of the network traffic content does not match the prescribed type; and

a second processor associated with the stack, wherein the second processor is configured to determine whether the network traffic content contains the content desired to be detected if the type of the network traffic content matches the prescribed type.

2. (Previously Presented) The device of claim 1, wherein the first processor comprises a general purpose processor.

3. (Previously Presented) The device of claim 1, wherein the first processor comprises an ASIC processor.

4. (Original) The device of claim 3, wherein the ASIC processor is a semi-custom ASIC processor.

5. (Original) The device of claim 3, wherein the ASIC processor is a programmable ASIC processor.

6. (Previously Presented) The device of claim 1, wherein the first processor is further configured to send the network traffic content to a user when the protocol of the network traffic content does not match the prescribed protocol.

7. (Original) The device of claim 1, further comprising the stack.

8. (Previously Presented) The device of claim 7, wherein the stack is implemented in the first processor or in the second processor.

9. (Previously Presented) The device of claim 8, wherein the stack is configured to store the network traffic content in accordance with the protocol of the network traffic content.

10. (Previously Presented) The device of claim 1, wherein the first or the second processor is further configured to assemble the at least a portion of the network traffic content with the rest of the network traffic content, and transmit the network traffic content to a user when it is determined that the network traffic content does not contain the content desired to be detected.

11-12. (Canceled)

13. (Previously Presented) The device of claim 1, wherein the second processor comprises an ASIC processor.

14. (Previously Presented) The device of claim 1, wherein the first or the second processor is further configured to flag the network traffic content when the protocol of the network traffic content matches the prescribed protocol, and send the flagged network traffic content to a memory.

15-16. (Canceled)

17. (Previously Presented) The device of claim 14, wherein the second processor comprises an ASIC processor.

18. (Original) The device of claim 1, wherein the content desired to be detected is selected from the group consisting of a virus, a worm, a web content, a Trojan agent, an email spam, and a packet transmitted by a hacker.

19. (Previously Presented) A method for managing network traffic flow, the method comprising:

receiving network traffic content at a first processor;

determining whether a protocol of the network traffic content matches with a prescribed protocol of network traffic content that could contain content desired to be detected by comparing a type of the network traffic content with a prescribed type;

performing filtering of the network traffic by the first processor if the type of the network traffic content does not match the prescribed type;

storing the network traffic content in a stack when the protocol of the network traffic content matches the prescribed protocol, the stack associated with a module including a second processor that is configured to determine whether the network traffic content contain content desired to be detected if the type of the network traffic content matches the prescribed type; and

sending at least a portion of the network traffic content to a memory when the protocol of the network traffic content matches the prescribed protocol;

wherein the first and second processors are parts of a device.

20. (Original) The method of claim 19, wherein the network traffic content is stored in the stack in accordance with the protocol of the network traffic content.

21. (Previously Presented) The method of claim 19, further comprising:

assembling the at least a portion of the network traffic content with the rest of the network traffic content, and sending the network traffic content to a user when it is determined that the network traffic content does not contain the content desired to be detected.

22. (Previously Presented) The method of claim 19, further comprising:

flagging the network traffic content when the protocol of the network traffic content matches the prescribed protocol; and

storing the flagged network traffic content in a memory.

23-26. (Canceled)

27. (Previously Presented) A device for managing network traffic flow, the device comprising:

a first processor, the first processor configured to

receive network traffic content,

flag the network traffic content by inserting data or modifying a portion of the network traffic content,

send the flagged network traffic content to a module, the module configured to pass unflagged data to a user and prevent flagged data from being sent to the user, and

send a copy of the network traffic content to a second processor, the second processor configured to determine whether the network traffic content contains content desired to be detected; and

the second processor.

28. (Original) The device of claim 27, wherein the first processor is further configured to transmit the network traffic content to a user when it is determined that the network traffic content does not contain the content desired to be detected.

29. (Original) The device of claim 27, wherein the module comprises a memory, a buffer, or at least a portion of a processor.

30. (Previously Presented) A method for managing network traffic flow, the method comprising:

receiving network traffic content at a first processor;

flagging the network traffic content by inserting data or modifying a portion of the network traffic content;

sending the flagged network traffic content to a module, the module configured to pass unflagged data to a user and prevent flagged data from being sent to the user; and

sending a copy of the network traffic content to a second processor, the second processor configured to determine whether the network traffic content contains content desired to be detected;

wherein the first and second processors are parts of a device.

31. (Original) The method of claim 30, further comprising transmitting the network traffic content to a user when it is determined that the network traffic content does not contain the content desired to be detected.

32. (Previously Presented) The device of claim 1, further comprising a memory coupled to the first processor.

33. (Previously Presented) The device of claim 27, wherein the first processor is configured to pass a portion of the network traffic content downstream before the second processor finishes processing the network traffic content.

34. (Previously Presented) The device of claim 27, wherein the first processor and the second processor are parts of a processor.

35. (Previously Presented) The device of claim 34, wherein the processor comprises an ASIC processor.

36. (Previously Presented) The device of claim 27, wherein the first processor is configured to flag the network traffic content by modifying data associated with the network traffic content or by inserting data to the network traffic content.

37. (Previously Presented) The method of claim 30, wherein a portion of the network traffic content is passed downstream before the processor finishes processing the network traffic content.

38. (Previously Presented) The method of claim 30, wherein the second processor comprises an ASIC processor.

39. (Previously Presented) The method of claim 30, wherein the network traffic content is flagged by modifying data associated with the network traffic content or by inserting data to the network traffic content.

40-42. (Canceled)

43. (New) The device of claim 1, wherein the content desired to be detected is undesirable content.

44. (New) The method of claim 19, wherein the content desired to be detected is undesirable content.

45. (New) The device of claim 27, wherein the content desired to be detected is undesirable content.

46. (New) The method of claim 30, wherein the content desired to be detected is undesirable content.

47. (New) The device of claim 14, wherein the memory is cleared of the flagged network traffic content after operation on the data has completed.

48. (New) The method of claim 22, further comprising:

clearing the network traffic content from the memory.

49. (New) The device of claim 14, wherein flagging the network traffic content indicates that the data may contain undesirable content.

50. (New) The method of claim 22, wherein flagging the network traffic content indicates that the data may contain undesirable content.

51. (New) The device of claim 27, wherein flagging the network traffic content indicates that the data may contain undesirable content.

52. (New) The method of claim 30, wherein flagging the network traffic content indicates that the data may contain undesirable content.

53. (New) The device of claim 1, wherein determining whether a protocol of the network traffic content matches a prescribed protocol of network traffic content that could contain content desired to be detected further includes:

comparing a port over which the network traffic content was received with preassigned ports to determine the type of content being screened.

54. (New) The method of claim 19, wherein determining whether a protocol of the network traffic content matches with a prescribed protocol of network traffic content that could contain content desired to be detected further includes:

comparing a port over which the network traffic content was received with preassigned ports to determine the type of content being screened.

55. (New) The device of claim 27, wherein the second processor is configured to determine whether the network traffic content contains content desired to be detected by:

comparing a port over which the network traffic content was received with preassigned ports to determine the type of content being screened.

56. (New) The method of claim 30, wherein the determining whether the network traffic content contains content desired to be detected performed by the second processor includes:

comparing a port over which the network traffic content was received with preassigned ports to determine the type of content being screened.

57. (New) The device of claim 1, wherein at least one of the first processor and the second processor are configured to decrypt the network traffic content.

58. (New) The method of claim 19, further comprising:

decrypting the network traffic content.

59. (New) The device of claim 27, wherein at least one of the first processor and the second processor are configured to decrypt the network traffic content

60. (New) The method of claim 30, further comprising:

decrypting the network traffic content.